CLAIMS

We claim:

1. A method for determining the presence of an anomaly region in a digital medium comprising:

performing multiple read operations on a data segment of the medium to generate multiple corresponding read data results;

calculating corresponding digital signatures for each of the multiple read data results; and

determining whether an anomaly region is present in the data segment based on a comparison of the digital signatures.

2. The method of claim 1 wherein the data comprises data selected from the group consisting of: user data, error data, sync data, parity data, header data, and sub-channel data.

3. The method of claim 1 further comprising monitoring a transfer rate of the read data during at least one of the read procedures, and further determining whether an anomaly region is present in the data segment based on the monitored transfer rate.

4. The method of claim 1 further comprising:

first monitoring a first transfer rate of first read data during one of the read procedures, and further determining whether an anomaly region is present in the data segment based on the monitored first transfer rate; and

in the event that the presence of an anomaly is not determined as a result of the first monitoring, second monitoring a second transfer rate of second read data during another of the read procedures, and further determining whether an anomaly region is present in the data segment based on the monitored second transfer rate.

5. The method of claim 1 wherein calculating corresponding digital signatures for each of the multiple read data results comprises calculating a digital signature selected from the group

consisting of MD2, MD4, MD5, Snefru, SHA, NIST DSA, Haval, N-Hash, and RIPE-MD digital signatures.

6. The method of claim 1 wherein determining whether an anomaly region is present in the data segment of the medium based on a comparison of the digital signatures comprises determining whether the any of the digital signatures are equal in value.

7. The method of claim 6 further comprising, if none of the digital signatures are equal in value, determining the anomaly region to be present.

8. The method of claim 6 further comprising, if a predetermined number of the digital signatures are not equal in value, determining the anomaly region to be present.

9. The method of claim 1 further comprising authenticating the medium in response to the determination of the presence of the anomaly region.

10. A system for determining the presence of an anomaly region in a digital medium comprising:

a read unit for performing multiple read operations on a data segment of the medium to generate multiple corresponding read data results;

a calculating unit for calculating corresponding digital signatures for each of the multiple read data results; and

a determining unit for determining whether an anomaly region is present in the data segment based on a comparison of the digital signatures.

11. The system of claim 10 wherein the data comprises data selected from the group consisting of: user data, error data, sync data, parity data, header data, and sub-channel data.

12. The system of claim 10 further comprising a rate monitoring unit for monitoring a transfer rate of the read data during at least one of the read procedures, and further determining whether an anomaly region is present in the data segment based on the monitored transfer rate.

13. The system of claim 10 further comprising:

a monitoring unit for first monitoring a first transfer rate of first read data during one of the read procedures, and further determining whether an anomaly region is present in the data segment based on the monitored first transfer rate; and, in the event that the presence of an anomaly is not determined as a result of the first monitoring, second monitoring a second transfer rate of second read data during another of the read procedures, and further determining whether an anomaly region is present in the data segment based on the monitored second transfer rate.

14. The system of claim 10 wherein the calculating unit calculates a digital signature selected from the group consisting of MD2, MD4, MD5, Snefru, SHA, NIST DSA, Haval, N-Hash, and RIPE-MD digital signatures.

15. The system of claim 10 wherein the determining unit determines whether the any of the digital signatures are equal in value.

16. The system of claim 15 wherein, if none of the digital signatures are equal in value, the anomaly region is determined to be present.

17. The system of claim 15 wherein, if a predetermined number of the digital signatures are not equal in value, the anomaly region is determined to be present.

18. The system of claim 10 further comprising means for authenticating the medium in response to the determination of the presence of the anomaly region.